Generator liczb losowych

Pawel Pycinski

Uniwesytet Jagielloski

TABLE OF CONTENTS

1 Wprowadzenie

2 Sposoby generowania liczb pseudolosowych

3 Wasny generator

4 Sources

Cel Projektu

Celem projektu jest stworzenie generatora całkowitych liczb pseudolosowych o rozkładzie równomiernym. Na podstawie stworzonego generatora należy stworzyć generatory o rozkładzie jednostajnym (na przedziale [0,1]), Bernoulliego, dwumianowego, Poissona, wykładniczego i normalnego. Następnie należy przetestować powstałe generatory.

Definicja

Generator liczb pseudolosowych – program lub podprogram, który na podstawie niewielkiej ilości informacji generuje deterministycznie ciąg bitów, który pod pewnymi względami jest nieodróżnialny od ciągu uzyskanego z prawdziwie losowego źródła.

Generator liczb pseudolosowych nie bez powodu jest **pseudolosowy**, problem z otrzymaniem liczb losowych wynika z deterministycznego charakteru komputera i wykonywanych przez niego operacji. Gdy człowiek dokonuje rzutu kością, nie wie co wypadnie. Taka sama operacja na komputerze wymaga działania, którego wynik jest nieprzewidywalny – żadna z operacji wykonywanych przez procesor nie posiada takiej cechy.

Problem starano się rozwiązać wykorzystując zewnętrzne źródła sygnałów losowych (np. generatory białego szumu), jednakże w tego typu urządzenia nie są standardowo wyposażano komputery osobiste. Próbowano także wykorzystać szumy kart dźwiękowych, jednakże system ten nie rozpowszechnił się z prostej przyczyny – różne karty dźwiękowe szumią różnie, a te z górnej półki nie szumią prawie wcale.

Sposoby generowania liczb pseudolosowych

Jest wiele sposobów generowania liczb pseudolosowych. Jedną z grup generatorów są generatory liniowe. tworzą ciąg liczb według schematu:

$$X_{n+1} = (a_1 X_n + a_2 X_{n-1} + \ldots + a_k X_{n-k+1} + c) \mathrm{mod}(m)$$

gdzie a_1,...,a_k, c, m -parametry generatora (ustalone liczby)

Generatory używające operacji modulo nazywamy **kongruencyjnymi**. Każdy kolejny wyraz (liczba pseudolosowa) w generatorze liniowym to suma pewnych poprzednich wyrazów pomnożonych każdy z każdą o jakiś skalar i brane z nich jest modulo.

Generator mulitplikatywny tworzy liczby według schmatu:

$$X_{i+1} = (aX_i + c) \mathrm{mod}(m) \iff c = 0$$

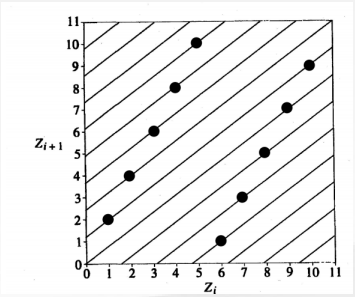
Kolejny wyraz tworzymy po przez pomnożenie poprzedniego przez jakiś skalar. Gdy $c \neq 0$ to generator jest kongurentnie mieszany.

Wasny generator

Swój generator postanowiłem zbudować na bazie generatora mulitplikatywnego. Jest to jeden z łatwiejszych generatorów, prosty do implementacji.

Posiada on niestety dwie poważne wady:

1. Gererator generuje liczby ciągu w sposób deterministyczny przez co łatwo jest wyliczyć kolejną liczbę.
2. Wybierając złe czynniki możemy spowodować, że okres generatora będzie mały przez co będzie działał niepoprawnie lub będzie generował bardzo mało liczb losowych.
3. Generowane liczby lokalizują się na hiperpłaszczyznach, których położenie uzależnione jest od parametrów generatora.



Przez wyżej wymienione czynniki nie może być on stosowany w kryptografii.

Wasny generator

Przed zaimplementowaniem pozostał jeszcze wybór m oraz a dla naszego generatora.

Niech $\mathrm{m} = 2^{32}$, jest to liczba o 1 większa od zakresu unsigned int'a, dzięki czemu nasza kongruencja potencjalnie będzie mogła zwracać wszyskie liczby które jesteśmy w stanie zapisać na 4 bajtach int'a.

Sources

- http://home.agh.edu.pl/~chwiej/mn/generatory_16.pdf
- https://pl.wikipedia.org/wiki/Generator_liczb_pseudolosowych
- https://eduinf.waw.pl/inf/alg/001_search/0022.php